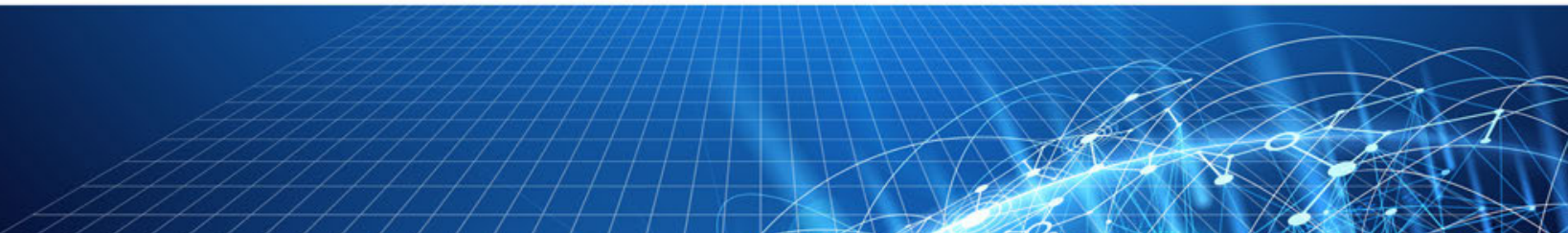
DEFENSE SECURITY ENTERPRISE ARCHITECTURE

Closing Information Sharing and Security Gaps for the Department of Defense

Product Reference Guide

Revision 1.0

June 2016



CONTENTS

FIGURES

TABLES

1 Introduction

The need to improve information-sharing capabilities across all five primary Defense Security Enterprise (DSE) domains (i.e., physical, personnel, industrial, information, and operational) has been tragically highlighted by events such as the shootings at Fort Hood, TX, in November 2009, at the Washington Navy Yard, DC, in September 2013, again at Fort Hood in April 2014, and most recently the shootings in Chattanooga, TN. Currently, defense security information sharing requests are sent manually via email, telephone calls, PowerPoint briefings, and other non-automated processes. These are neither effective nor efficient methods of accessing defense security-related information. This information is available within the DSE domains and must be readily accessible to prevent, protect, mitigate, or respond to security-related incidents. When the aforementioned events occurred, neither installations in the surrounding area nor U.S. Northern Command (USNORTHCOM) were notified. Had any of these shootings been part of a coordinated attack, U.S. installations were unprepared to prevent, protect, mitigate, or respond to another simultaneous or secondary incident. This lack of preparedness directly impacts broader mission assurance interests, goals, and objectives.

2 Mission

In August 2013, the Defense Security Enterprise Advisory Group (DSEAG) chartered a Physical Security Enterprise and Analysis Group (PSEAG)-funded project to create the Defense Security Enterprise Architecture (DSEA) solution that will leverage research and development efforts and functional requirements to provide an information sharing capability across all defense security domains. The objective is to allow information to flow within and across the five primary defense security disciplines—physical, personnel, industrial, information, and operational—honoring information sensitivity, and disseminating relevant information to areas where it can have the greatest impact and improve the effectiveness and efficiency of decision makers. The DSEA Project Team is designed to provide continuous support to enhance military installation access control, hazard and threat situational awareness, emergency management, force protection information sharing and operational execution efforts through information access, collaboration, analysis, and dissemination. Further, it is the intent of the DSEA Project Team to create a software framework able to pass automated near real-time information within a selected demonstration environment.

3 Solution

The DSEA-Backbone is a Joint Office of the Secretary of Defense (OSD) Research and Development (RDT&E) initiative addressing vertical and horizontal information sharing across the DSE domains, missions, and functions (e.g., Special Access Program security policy, critical program information protection policy, and security training). The plan is to

align with counterintelligence, information assurance, foreign disclosure, security cooperation, technology transfer, export control, cyber security, nuclear physical security, chemical and biological agent surety and security, antiterrorism, force protection, and mission assurance policy.

****Note that DSEA is not a Common Operating Picture (COP), does not replace a COP, or any end-point systems. DSEA is an integration, routing and mediation platform for data and information exchange across the Defense Security Enterprise.**

The DSEA-Backbone delivers a systems-level information sharing architecture that integrates and correlates all available and relevant security domains' authoritative data sources (ADS). This increased, automated, timely information sharing will directly improve authorized stakeholders' ability to identify, deny access to, and apprehend insider or external threats targeting Department of Defense (DoD) installations or assets. Additionally, the DSEA-Backbone can access and automatically distribute large volumes of all-threat indicators and warning data across unclassified domains in near real-time for improved situational awareness, protection, and threat mitigation. This capability is based on authorities and legal responsibilities to ensure data received by analysts meets user-specified criteria. This advancement in information sharing is made possible due to the ability of the DSEA to support information sharing among virtually any system or software program of record without forcing stakeholders to divest from existing legacy systems, software, or procedures, thereby providing users with a significantly enhanced information sharing capability at a negligible cost.

FIGURE 1. THE DSEA VISION—TRANSFORMING A COMPLEX, ERROR-PRONE SYSTEM OF AD HOC RELATIONSHIPS WITH INCONSISTENT PROTOCOLS AND INADEQUATE SECURITY TO A CENTRALIZED, STREAMLINED NETWORK OF INFORMATION SHARING SYSTEMS WITH A STRONG SECURITY MODEL, MANAGED QUALITY OF SERVICE, AND THE FACILITATION AND SUPPORT OF A HELP DESK.

4 Purpose

The DSEA-Backbone will allow for information sharing across communities that do not normally share data. Further, the intent is to provide, when appropriate, fused products to **allow decision makers to mitigate the impacts of adverse defense security events or prevent them from occurring**.

This document defines the products that the DSEA Project team has developed so that the software services and lessons learned can be leveraged for future programs within this domain space or tangential domain spaces.

5 Transition Objectives

As an enterprise capability that will meet the requirements of the warfighter, the Defense Information Systems Agency (DISA) is the logical hosting platform for the DSEA-Backbone capability, also known as the Defense Security Enterprise Environment (DSEE).

The transition objectives for the DSEA project are to:

- Develop a defense security and enterprise services infrastructure and determine transition partners early in the DSEA development process, for all defined capabilities and products
- Determine transition partners willing to provide long-term ownership, sustainment and future upgrades within their departments, agencies or program offices. These sustainment costs need to be appropriately estimated and agreed to by the DSEA leadership and the potential sustainment organizations
- Assist transition partners in defining the gaps in their current capabilities, especially for the stated needs of the DSEA
- Obtain acceptance of the transition by the sustaining organizations

Deliverables

- Enterprise architecture capability inclusive of an enterprise service bus providing an initial set of web services capable of conducting systems level information sharing (DSEA)
- Software services with appropriate documentation that can be reused or repurposed by the Federal Security Enterprise
- All appropriate technical demonstrations (TD), operational demonstrations (OD), and independent military utility assessment (MUA) reports
- Transition agreements (TA) with primary stakeholders

6 Transition Acceptance Events

6.1 DSEA Technical Demonstration (TD) #1 – 28 January 2015

Overview

The DSEA Technical Demonstration 1 (TD #1) took place 28 January 2015 in the Smart Center at Joint Base Andrews, Maryland. TD #1 utilized various use cases to set up scenarios in which the DSEA's information-sharing capabilities demonstrated the potential for an increase in decision-making effectiveness and efficiency. Points of integration were determined by examining each use case against a set of information points required to execute each scenario:

- Enumerating external systems required to execute
- Capabilities supported external protocols and exchange models
- Enumerating requirements on the DSEA backbone
- Service requirements (evaluating build/buy/adapt on each requirement)
- External system connection requirements
- Network topology (Virtual Private Network [VPN] connections, message protocols)

TD #1 Use Case Objectives

Use Case 1

Objective of Use Case 1 – Provide near real-time emergency management (EM) information across the Defense Security Enterprise and share this information with other government agencies as needed. Incidents of catastrophe and mass casualty required notifications and alerts sent to a broad spectrum of respondents across DoD, Department of Homeland Security (DHS), Department of State (DOS), and state/local entities.

Use Case 2

Objective of Use Case 2 – Provide real-time validation of current credentials for the purposes of access to DoD and/or DHS facilities. The scenario was created to demonstrate the capability of the DSEA to validate credentials across departments, as well as expand the attribute-based access available to government entities.

Use Case 3

Objective of Use Case 3 – Vet contract role players, cultural advisors, and linguists (CRP/CA/L) against appropriate authoritative data repositories (ADRs) of impeaching information to ensure they have no terrorist associations or adverse activity in their background history. This scenario was generated to establish the ability of the DSEA to ensure true and correct identity information is provided to those ADRs for matching, utilizing biometric identity information, and allowing for an informed real-time risk assessment.

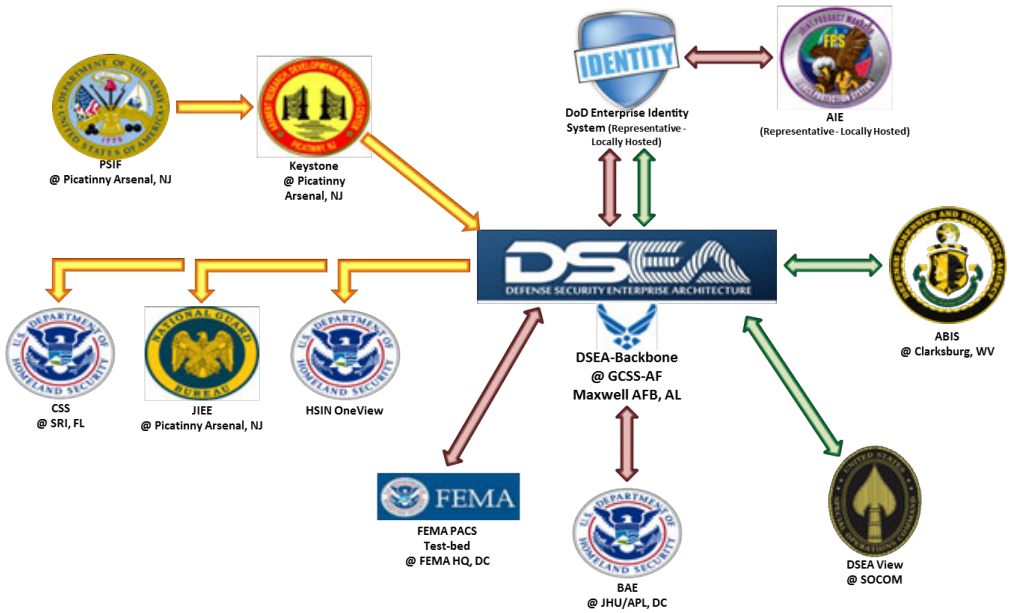


FIGURE 2A. DSEA TECHNICAL DEMONSTRATION #1 COMPOSITE (INFORMATION SHARING FROM USE CASES 1, 2, AND 3)

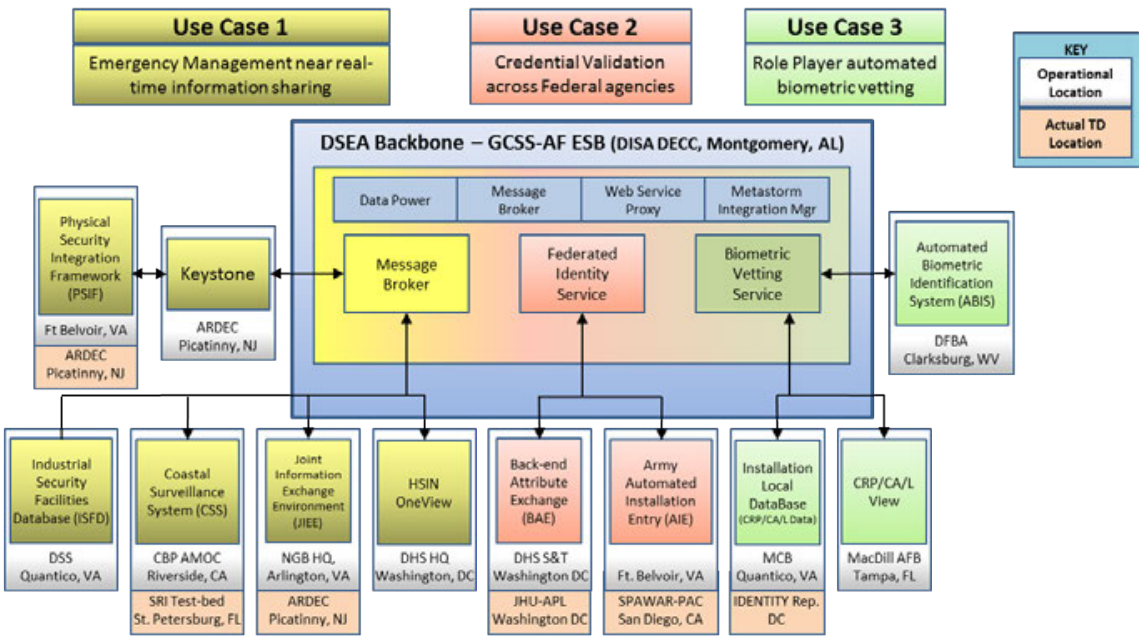


FIGURE 2B. DETAILED SCHEMATIC OF DSEA TECHNICAL DEMONSTRATION #1 INFORMATION SHARING FROM USE CASES 1, 2, AND 3 HIGHLIGHTING THE EXISTING SYSTEMS UTILIZED AND HOW THEY DEMONSTRATE THE POTENTIAL INTEGRATION POINTS AND VALUE ADDED OF THE PROPOSED INFORMATION SHARING FLOW.

Results

The aim of TD-1 was to show the technical feasibility and initial utility of sharing information across the Defense Security Enterprise. While the use cases developed were

artificial, they were based on a combination of real-life events that the enterprise has faced. To that end, the event at the Smart Center successfully validated the objectives of the demonstration. Further, it amplified a key requirement for the next technical development. While there is value added in sharing information across all security pillars in the Defense Security Enterprise, sometimes it will be necessary to redact information based on a need to know and responsibility of the position.

6.2 DSEA Technical Demonstration (TD #2) – 17 November 2015

Overview

The DSEA Technical Demonstration 2 (TD #2) took place 17 November 2015 in the Smart Center at Joint Base Andrews, Maryland. TD #2 utilized new use cases to further establish DSEA's information-sharing capabilities and continue to demonstrate the effects of access to near real-time, relevant information. The focus of TD #2 was on the ability to make informed, timely decisions to prevent, protect, mitigate, or respond to a potential critical situation. TD #2 brought more than 40 executives and specialists together representing numerous DoD and DHS components and agencies.

TD #2 Use Case Objectives

DSEA TD #2 demonstrated four use case scenarios that demonstrated how information sharing through the DSEA Backbone connected the actions of three individuals who were attempting to obtain access to USG agencies and systems to facilitate the theft and shipment of stolen weapons into a U.S. port.

Use Case 1

Objective of Use Case 1 – Joint Interagency Task Force South (JIATF-S) administrator requests biometric vetting for a potential new employee. Administrator initiates vetting process via the DSEA, specifically checking for human rights violations or other questionable background history. The response from the DSEA is that the person in question is associated with an illegal narcotics trafficking cartel.

Use Case 2

Objective of Use Case 2 – Identity Matching Engine for Security and Analysis (IMESA) credential validation for a Common Access Card (CAC) holding member of the janitorial staff at SSC Pacific. Credential validation initiated via the DSEA indicated that the person in question is associated with an illegal narcotics trafficking cartel. Results are in a detain code, CAC is revoked, and BOLO alert is generated.

Use Case 3

Objective of Use Case 3 - Suspicious activity report (SAR) intelligence received from the U.S. European Command (EUCOM) links outside the continental United States to continental U.S. threat information regarding an overseas package to be picked up by an unknown U.S. service member. The intelligence from EUCOM and biometric vetting (Use Case 1), plus access control (Use Case 2) provide indicators of a potential attack.

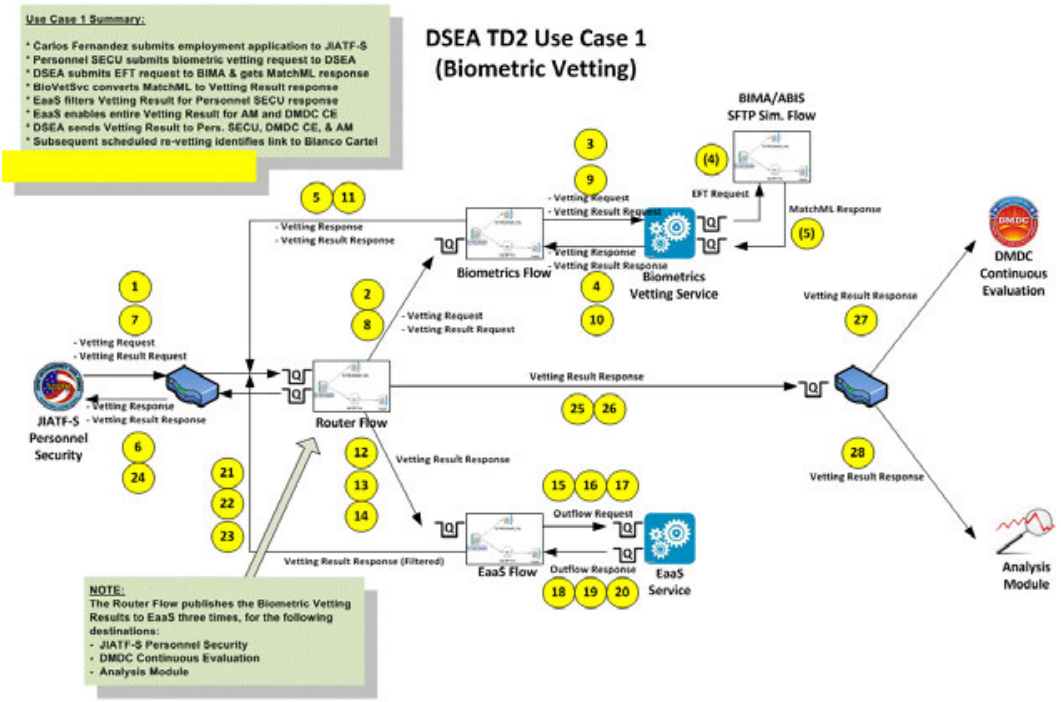


FIGURE 3A. DSEA TD #2 BIOMETRIC VETTING – JIATF-S USE CASE.

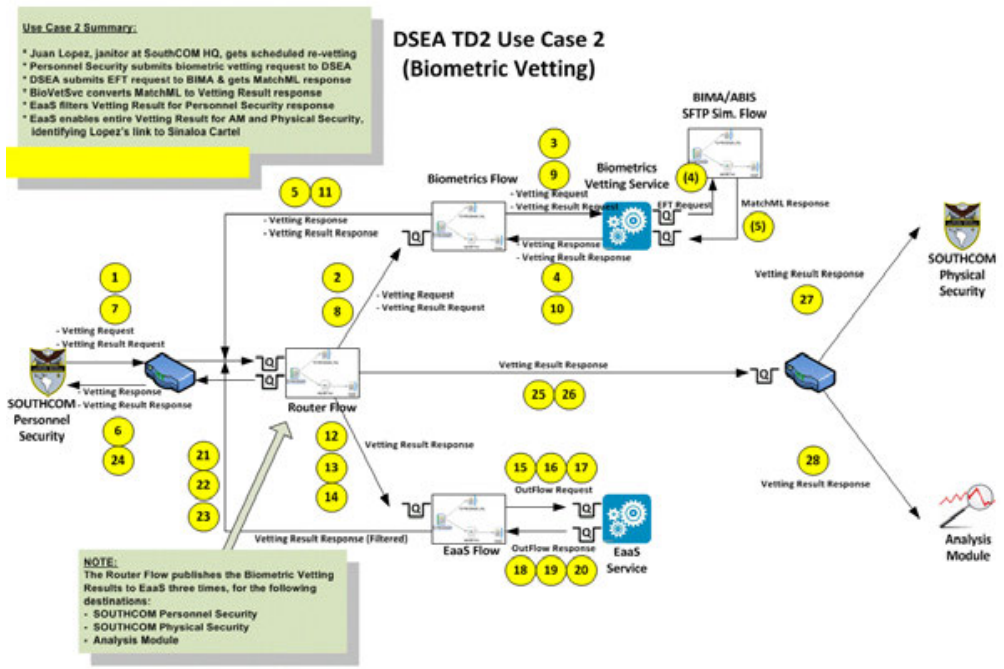


FIGURE 3B. DSEA TD #2 BIOMETRIC VETTING – SOUTHCOM USE CASE.

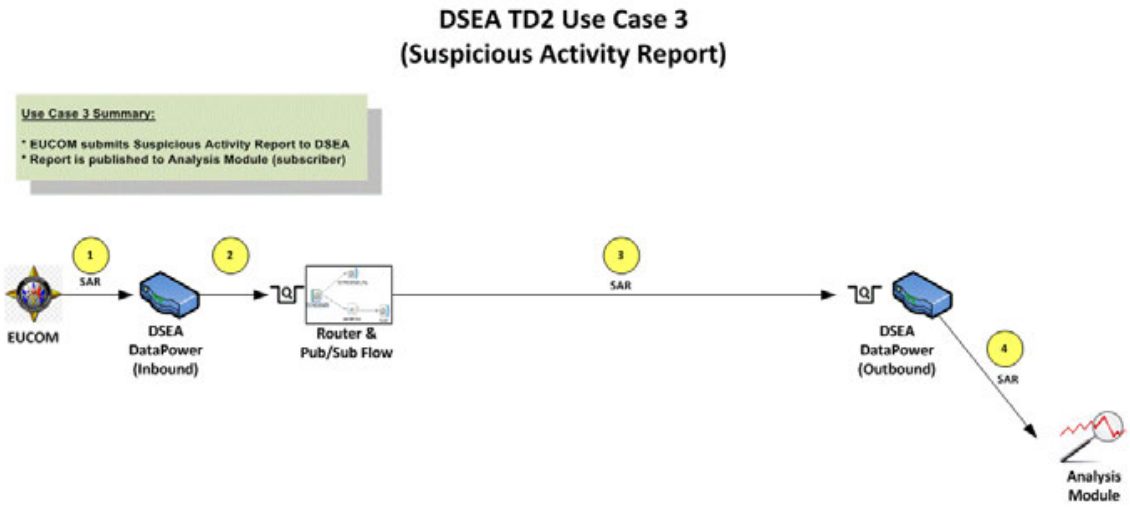


FIGURE 4. DSEA TD #2 SUSPICIOUS ACTIVITY REPORTING (SAR) USE CASE.

Use Case 4

Objective of Use Case 4 – Demonstrate the benefits of cross-department vetting. In the use case. a U.S. military service member approaches a Physical Access Control System (PACS) card reader at U.S. Customs and Border Protection office in San Diego, CA. The service member uses his DoD Common Access Card (CAC) in an attempt to obtain access, and his credential validation information provided via DSEA indicates he has been Absent Without Official Leave (AWOL) for two weeks and has an association to other suspicious activities. Focus of the use case is on intelligence combined with biometric vetting and then access control. The DSEA generates alerts sent to the U.S. Customs and Border Protection office in San Diego, CA, and to pertinent agencies along the West Coast of the U.S. about the potential attack and the link to a suspicious package being picked up by an unknown service member. The local police and emergency management personnel are alerted and roads are cordoned, resulting in recovering and defusing of a bomb.

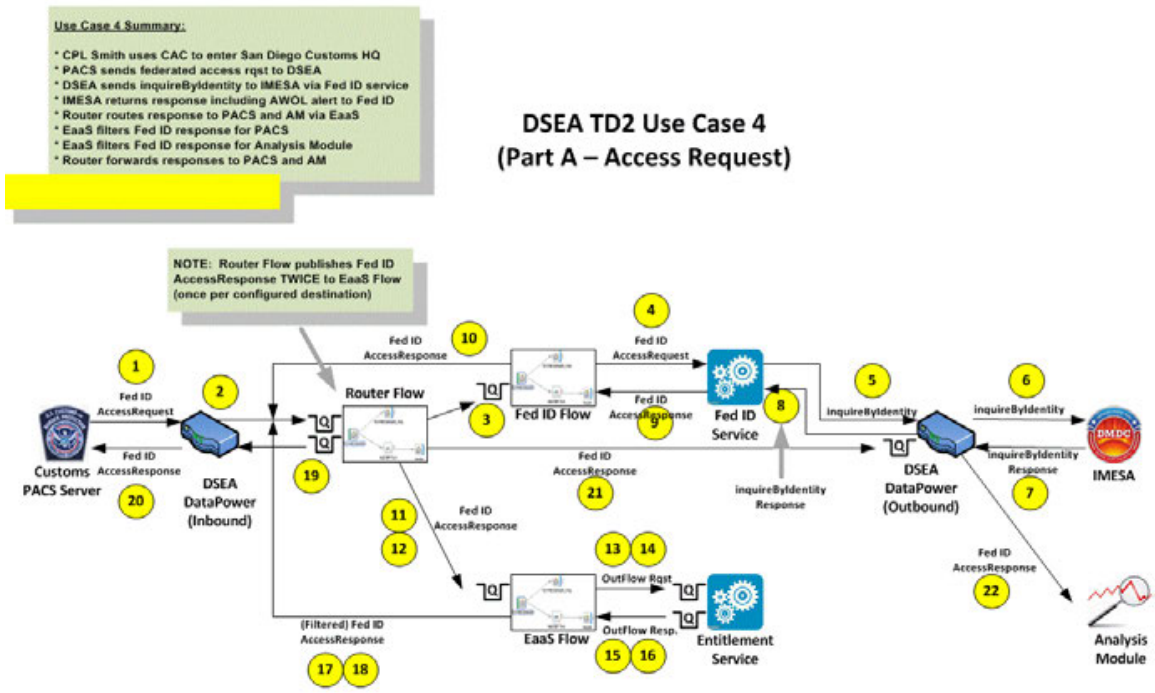


FIGURE 5. DSEA TD #2 ACCESS REQUEST USE CASE.

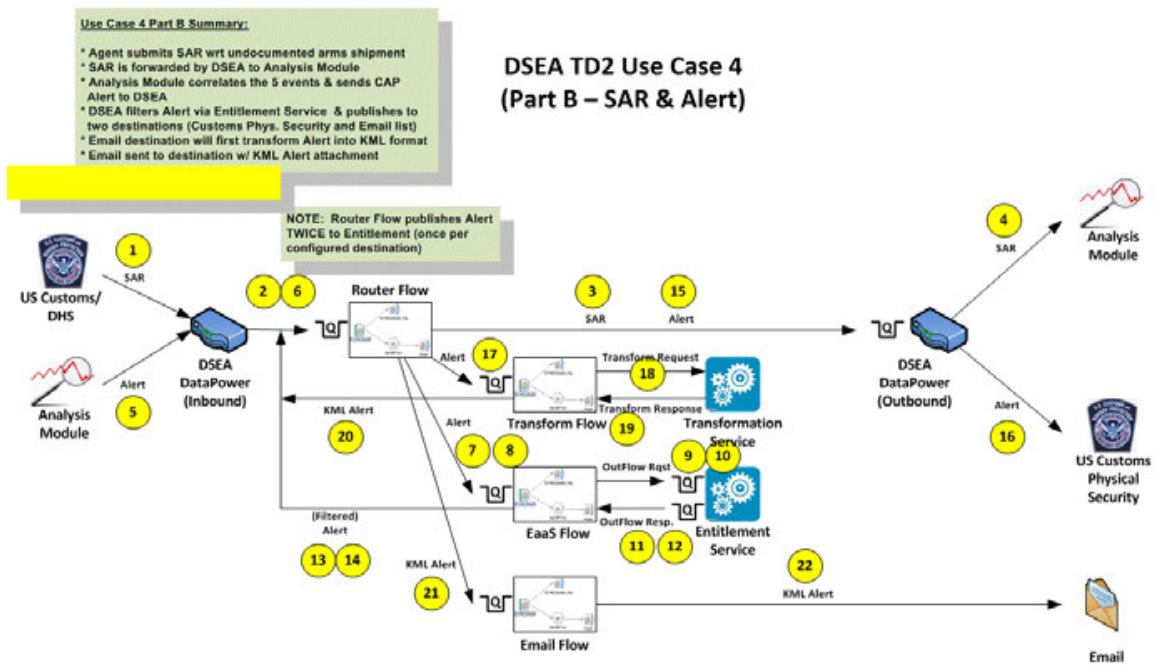


FIGURE 6. DSEA TD #2 SAR AND ALERT USE CASE.

Results

The objectives of TD #2 was to further demonstrate additional Defense Security use cases while showing the key requirements developed as a result of the feedback provided from TD #1. This feedback specified that managed information sharing is based on a need to know and authority in the situation. TD #2 successfully demonstrated this capability using Entitlements as a Service (EaaS), a redaction capability that the previous demonstration did not include. Further, the DSEA Project Team facilitated the technical management of suspicious activity reports (a key U.S. Army North (ARNORTH) requirement) and demonstrate the value of fusing some of this information together through a representative analysis module, allowing for decision makers to make more timely decisions.

Principal attendees stressed the importance of information sharing within and across the departments as essential and critical to reducing or preventing loss of life. The DoD chief information officer (CIO) voiced support of what DSEA is attempting to accomplish, and U.S. NORTHCOM reiterated that there are currently 10 information-sharing gaps across six unified combatant commands. Information sharing at an enterprise level across the major defense security functional areas is essential for achieving mission assurance. This method of information sharing should reside with a program that can maintain and sustain enterprise information sharing by promoting and enforcing policies and standards at all levels of government.

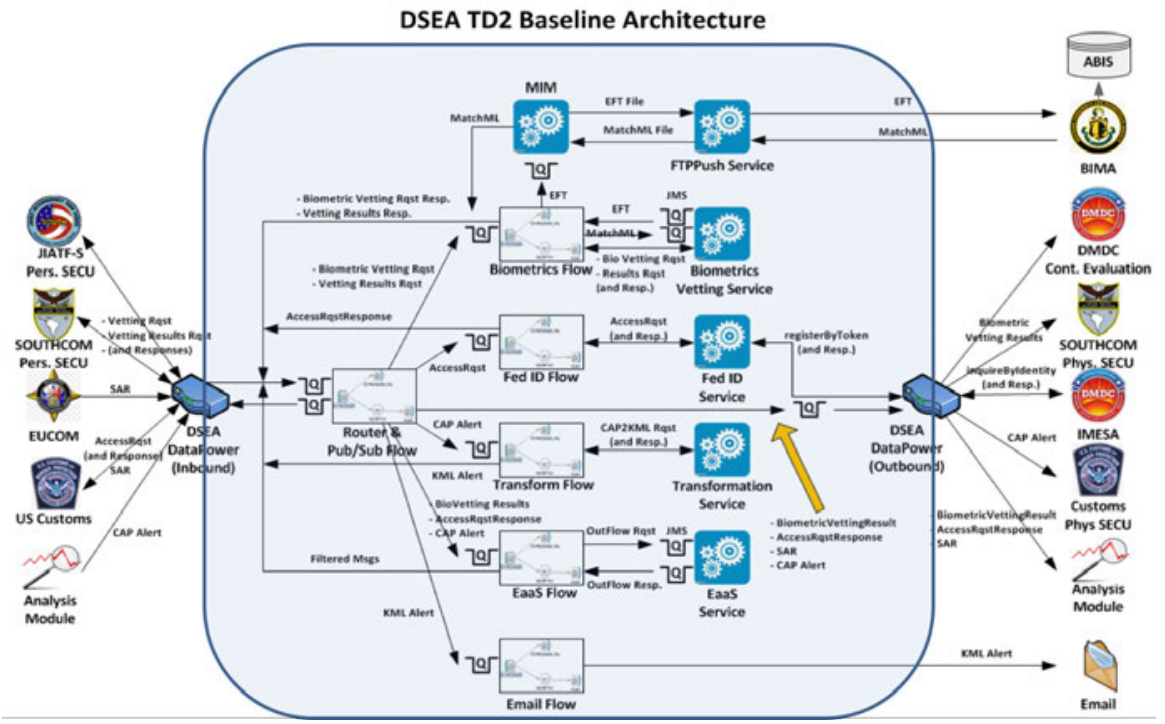


FIGURE 7. DSEA TD #2 TECHNICAL ARCHITECTURE OVERVIEW.

6.3 DSEA Functional Transition Demonstration (FXD) – 23-30 June 2016)

Overview

The DSEA Functional Transition Demonstration (FXD) will take place23–30 June 2016 in the Topside Conference Center at Space and Naval Warfare Systems Center Pacific in San Diego, CA. The FXD is planned as the culmination of the previous technical demonstrations, with multiple operational attributes. The intent is to utilize operational systems, data and operators (as possible), but not real or "live" networks. The objective is to ensure that the DSEA is in an appropriate transition-ready state. The FXD is designed to allow technology integration partners to test selected capabilities within the DSEA framework. The FXD approach will fully document and test the system to match many of the specifications that acquisition programs require, including functional, technical, and independent testing and assessments. Further, the FXD is intended to gather the key stakeholders and potential transition partners into a venue to demonstrate current capabilities and functionality that would be useful to each of them. This approach allows for the respective stakeholders to determine the value added of the transition of all or parts of the DSEA capability to their organization.

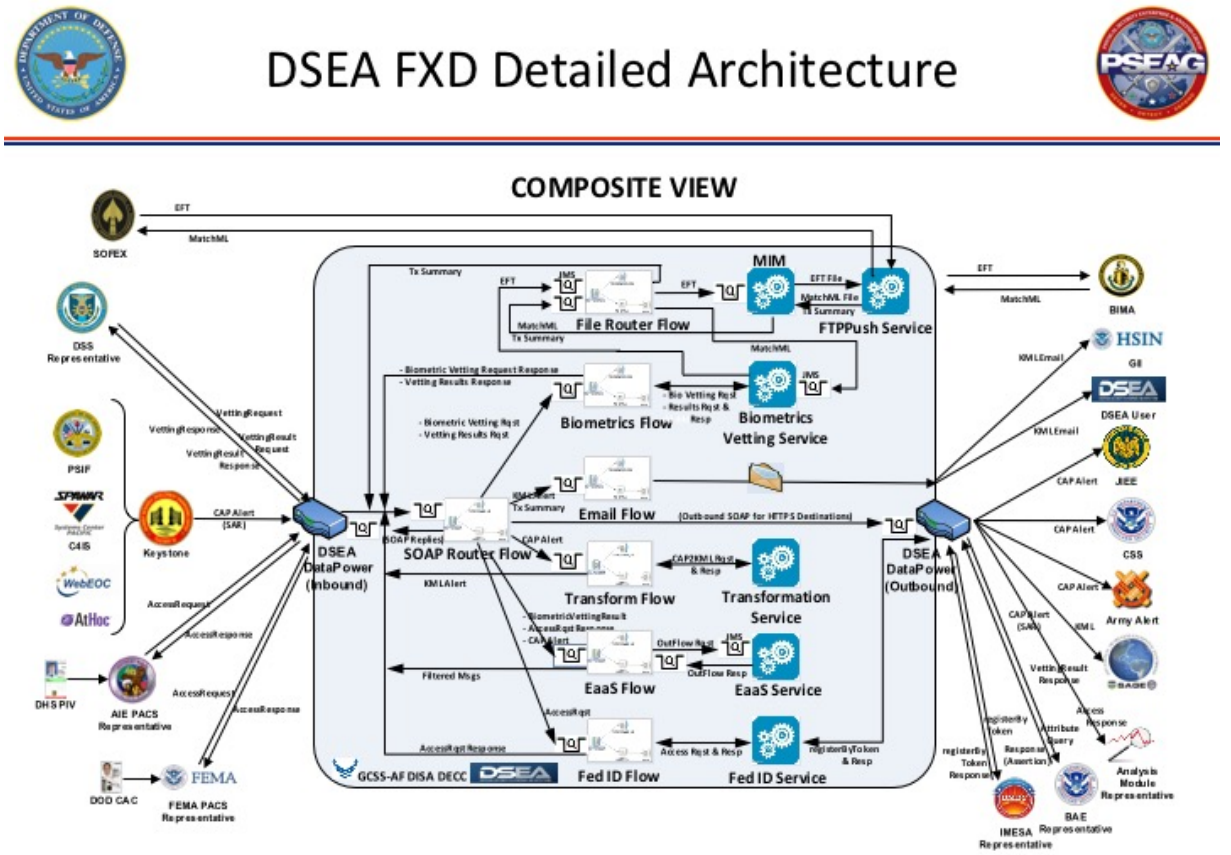


FIGURE 8. DSEA FXD DETAILED ARCHITECTURE (NOTIONAL).

Disclaimer: At the time of the publication of this report, the FXD planning was in-progress. Therefore, the descriptions and related information are written in the future tense, and the figures used are draft versions. As with the previous acceptance event, no "Results" are presented at this time. The result information will be captured in the test and assessment documentation following the event. For further information regarding the results of this event, please refer to the point of contact information in Table 2.

FXD Use Case Objectives

The FXD will be based on the use cases from TD #1 and TD #2, and will be organized as discrete use cases for the testing and assessment period. Information is as follows:

- Use Case 1: Emergency Management Alert Distribution
- Use Case 2: Biometric Vetting
- Use Case 3: Access Control/Federated ID
- Use Case 4: Suspicious Activity Reporting

The intention is to utilize these use cases into a final scenario for an FXD Capstone Demonstration that would be based on insider threat, and allow for information sharing to be demonstrated to the appropriate systems and role players.

Additionally, the use cases are updated to support SSC Pacific technology integration partners, including the Integrated Early Warning (IEW) Program to introduce a biological information thread, and the Army Alert Program to demonstrate information sharing among multiple mass notification systems communicating seamlessly. Finally, USNORTHCOM led, and the Defense Security and CBRN (chemical, biological, radiological, and nuclear) Analysis Team assisted in the development of the use cases and scenarios.

FXD Assessment Objectives:

The FXD will include an Independent Test and Assessment 23–27 June 2016. The results of the Test and Assessment will be provided in an initial utility assessment (UA) report within 30 days following the event.

As part of the lead up to the FXD assessment week, the DSEA Technical Management Team will provide the assessor with functional and software testing results, including software documentation artifacts providing details on the security testing and vulnerabilities, and any other findings related to the pre-production environment.

The discrete use case events will then become the test drivers for the assessor during the FXD assessment week. The assessor will also use information collected during the VIP day demonstration on 29 June 2016 as part of the report.

The goal of the technical assessment will be to identify the degree to which system capabilities support operational-like activities. Further, it will determine the degree to which technical documentation is available, complete, and accurate. Finally, a preliminary technology readiness level (TRL) will be recommended. The details of the preliminary TRL assessment will be available in the final UA report.

The goal of the software and functional assessment will be to evaluate and assess system functions in a laboratory environment, review code, databases, interface requirements, and architecture. Issues discovered during functional evaluation will be documented and potential risks will be identified. Issues from the FXD assessment week and VIP day demonstration events will be reported in the final UA report.

The plan is to collect survey information and feedback related to the potential operational usefulness of this capability during the VIP day demonstration. This feedback will be identified and documented in the UA report.

Results

None available. [At the time of the publication of this report, the FXD planning was in-progress. No "Results" are currently available. The results information will be captured in the UA report. For further information regarding the results of this event, please refer to points of contact information in Table 2.

7 DSEA Software Products and Services

The following capabilities are DSEA software products and services with a designation of "available for Transition", "infrastructure for Demonstration", or "endpoint data sharing system (for Demonstration)". The software components currently designated "available for Transition" are intended to be provided to SSC Pacific's technology and transition partners. [At the time of this report, the independent tests and assessments are just getting underway. The results of that testing and assessments will not be fully known or available until after the FXD event, and may impact the products and services available for transition.]

7.1 SIMON-based Services

SIMON is an open, extensible, standards-based, service-oriented architecture (SOA) platform developed by SRI International under contract to Naval Air Systems Command (NAVAIR). The SIMON platform enables rapid deployment of newly distributed systems and provides an integration platform for federating existing enterprise systems.

The non-proprietary SIMON platform enables an open marketplace of loosely coupled services that reduce integration expenses and vendor lock-in while increasing asset reuse and operational agility. SRI has developed numerous SIMON-based applications and systems for various USG entities, resulting in a suite of reusable services that can quickly be deployed for new applications like DSEA.

SIMON Alerting Service (DSEA Service Available for Transition)

The Alerting Collector Service is a centralized repository service for system-wide alerts. The service is primarily responsible for validating, logging, and collecting alerts provided by other systems and managing their activation and expiration. It will also provide the current list of active alerts to clients upon request.

The alerts themselves follow the Common Alerting Protocol (CAP) v1.1 alerting format, an OASIS standard used by the Department of Homeland Security, National Weather Service, and U.S. Geological Survey, and incorporated as a part of the National Information Exchange Model (NIEM), standardizes the alert format throughout the system.

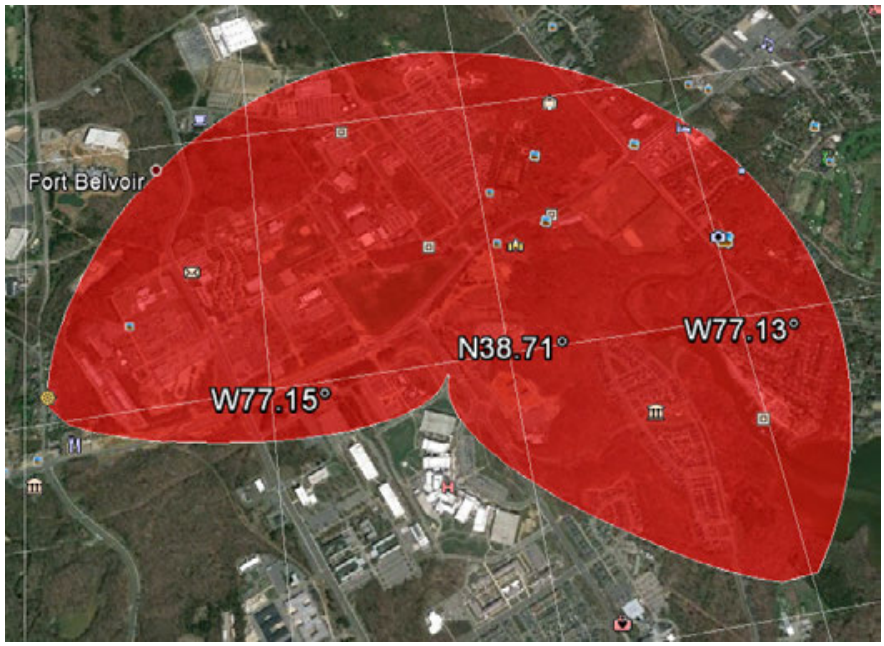


FIGURE 9. SCREENSHOT OF CAP ALERT TO KEYHOLE MARKUP LANGUAGE (KML).

The DSEA is compliant with existing systems of record in order to effectively relay security information. The Transformation Service is responsible for transforming data between disparate information exchange models (e.g., CAP and NIEM Alert Incident Association). The service supports declarative transformation models, allowing for rapid expansion to new exchange formats. The Transformation Service empowers DSEA to expand its information flow to communities as emerging needs arise.

SIMON Federated Identity Service (DSEA Service available for transition)

SIMON's Federated Identity Service was developed to consolidate information from as many identity providers as possible—from biometric matching to biographic vetting—to present the most complete and up to date identity of an individual. For DSEA, this service was configured to interact with multiple DoD and USG (DHS, Federal Bureau of Investigation [FBI], etc.) biometric and biographic identity providers to form a comprehensive view of a person of interest.

Entitlement as a Service (DSEA Service available for transition)

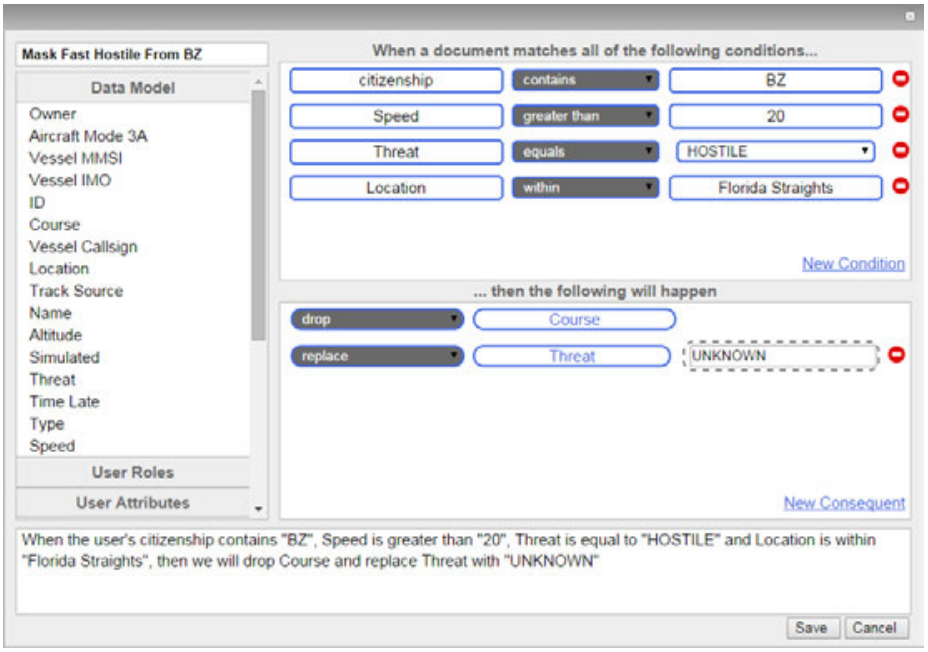


FIGURE 10. EAAS POLICY USER INTERFACE.

Entitlement is a core feature of SIMON that enables an authorized data administrator to control access to all elements of a data source based on the identity (role or attributes) of the requestor or other rules derived from a data access policy. Predefined (static) policy rules can be defined and stored and can be activated or deactivated dynamically. In addition, an authorized data administrator can define and activate complex access policy in real time. Entitlement has an accompanying user interface which simplifies definition and management of data access policies. Entitlement as a Service (EaaS) is a web service that has the same capabilities as SIMON Entitlement but can be deployed independently of a SIMON instance.

7.2 Global Combat Support System Air Force (GCSS-AF) Infrastructure Services (Infrastructure for Demonstration)

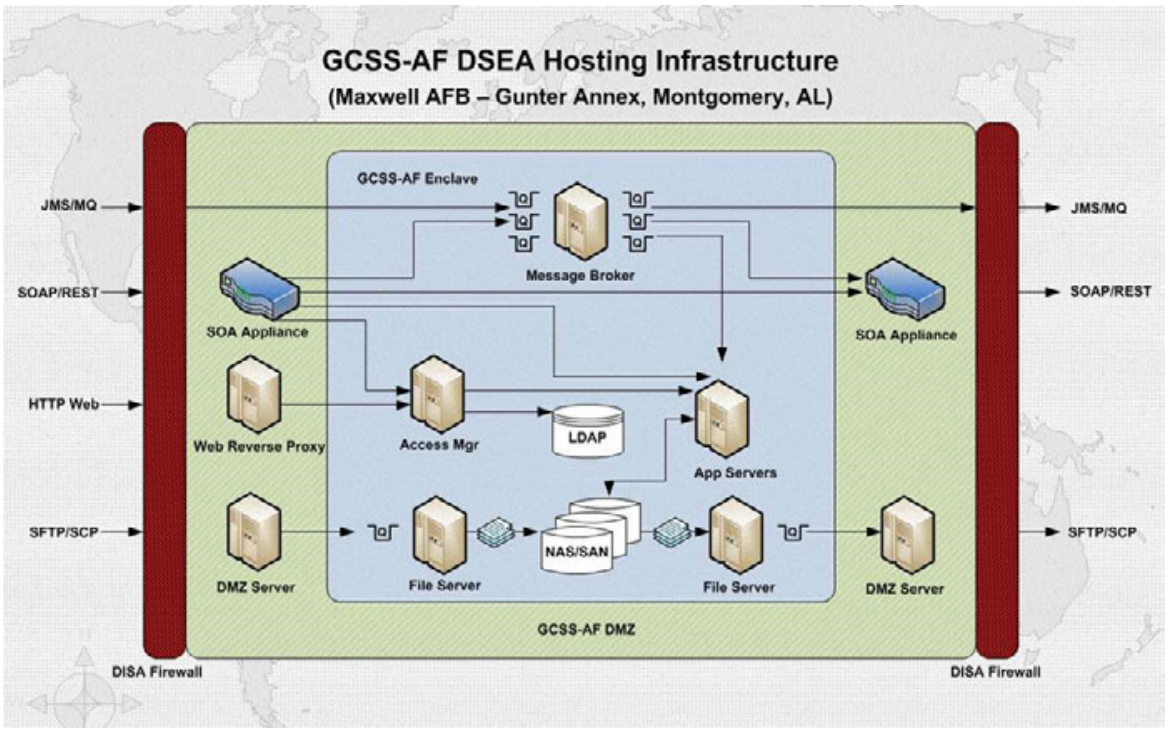


FIGURE 11. GCSS-AF DSEA HOSTING INFRASTRUCTURE.

Global Combat Support System–Air Force (GCSS-AF) is an enterprise computing environment for the U.S. Air Force featuring a common commercial off-the-shelf (COTS)-based infrastructure and security model that currently maintains the Air Force Portal (currently supporting more than 800,000 user accounts), hosts 33 mission applications, and protects more than 100 reduced sign-on applications that leverage the security layer behind the Air Force Portal. GCSS-AF resides within the DISA DECC (Defense Enterprise Computing Center) at the Gunter Annex of Maxwell AFB in Montgomery, AL, and has been operational since the early 2000s. In addition to hosting the aforementioned applications and services, GCSS-AF also serves as the conduit for integrating hundreds of applications/services, boasting over 1600 feeds/connections over a variety of technologies and protocols.

The following subsections describe the components of the GCSS-AF Messaging and Mediation service area that have been leveraged to support DSEA.

WebSphere DataPower (Infrastructure for Demonstration)

IBM® WebSphere DataPower is a hardened appliance for "bastion"-zone/DMZ push notification proxy of SOA message transactions originating outside of DSEA and GCSS-AF.

The primary function here is to provide secure access into the GCSS-AF Enclave, including the following:

- SSL endpoint services
- Payload encryption/decryption
- Public key infrastructure (PKI)-based digital signature
- Federal Information Processing Standard (FIPS) and DoD-compliant cryptography

Message integrity is also guaranteed via the above along with WSDL and XML schema compliance and enforcement.

In addition to protecting critical applications and services hosted within the DSEA with the above capabilities, the DataPower appliance also provides efficient and reliable multi-protocol transformation between connections (e.g., SOAP over HTTP to WebSphere MQ), thus enabling DataPower to integrate directly to the MQ-based enterprise service bus (ESB) backbone of GCSS-AF.

WebSphere MQ (Infrastructure for Demonstration)

IBM® WebSphere MQ is the primary messaging platform for supporting internal service-to-service communications within DSEA. Queue-based messaging enables loose coupling between senders and receivers while enabling reliability, persistence, transactionality, and quality of service. WebSphere MQ is known for its industrial-grade implementation. Synchronous communications, e.g., SOAP over HTTP, are typically susceptible to issues such as timeouts and data loss, as normally no mechanism for handling problems such as excessive network latency or system outages exist. However, the asynchronous messaging model of MQ, along with its support for transactionality, enables sending and receiving applications to ignore problems such as these, thus offering fault tolerance within unpredictable environments.

WebSphere Message Broker (Infrastructure for Demonstration)

IBM® WebSphere Message Broker is the core platform behind the GCSS-AF Enterprise Service Bus (ESB), enabling multi-protocol connectivity and complex processing and transformation capabilities among the components and applications/services attached to the ESB. Message Flows, the basic unit of deployment within Message Broker, are composed of building blocks known as nodes, where each node provides a configurable built-in functionality (e.g., sending/receiving protocol-specific messages, executing computer code, querying a database, performing XSL transformation, etc.). These nodes are sequentially tied together within a message flow as needed to provide the specific message processing and routing functionality necessary for any given integration, thus providing GCSS-AF with a powerful and flexible foundation for its ESB. Additionally, WebSphere MQ forms the backbone of the Message Broker, thus guaranteeing

reliable and predictable messaging within the ESB, along with supporting a variety of message distribution patterns, including request/response, one-to-many, many-to-one, and publication/subscription, etc.

Metastorm Integration Manager (Infrastructure for Demonstration)

OpenText MIM (formerly known as Metastorm Integration Manager) is a powerful integration platform for automating the movement of files between systems. Legacy systems and applications without the budgetary (and schedule) resources for re-engineering do not integrate well within existing service-oriented architectures. Therefore, file transferring is the only viable and expeditious solution for enabling these systems to integrate externally. MIM facilitates and automates this approach for integration by leveraging WebSphere MQ for reliable/transactional transfer of file data between systems/applications. MIM provides highly configurable components for managing file-to-queue and queue-to-file transformation and for managing directory-level monitoring and file transfer. Within GCSS-AF, MIM enables the ESB to integrate key file-based resources, including shared file systems and the File Transport Protocol (FTP) Push service.

GCSS-AF File Transfer Protocol (FTP) Push Service (Infrastructure for Demonstration)

FTP-Push is a service developed by GCSS-AF for automating legacy file transfers (via FTP, SFTP, and SCP) between GCSS-AF and external customer sites. File transfers are initiated from and delivered to specified directories, so all customizable configuration parameters (e.g., source/destination directory paths, user identification/password, retry count, name translations, etc.) are stored persistently in a database on a per-directory basis. The (multithreaded) FTP-Push service was designed around reliability and fault tolerance, so many configurable features support robust operations, including extensive retry logic, transactionality, a checksum file option, a time-stamped filename option, in-progress file names, and directory locking. Incoming (pulled and put) files are processed by the GCSS-AF anti-virus service, and FTP-Push is integrated with the GCSS-AF ESB via MIM.

7.3 Automated Biometric ID System (ABIS) – (Endpoint Data Sharing System)

ABIS is a quick reaction capability to support storing, matching, and sharing of collected biometric data primarily obtained during Operation Iraqi Freedom and Operation Enduring Freedom. DoD ABIS is an authoritative database that uses software applications to process and store biometrics modalities (i.e., fingerprints, palm prints, iris scans, and facial recognition data) from collection assets across the globe.

7.4 Automated Installation Entry (AIE) – (Endpoint Data Sharing System)

AIE is used to enhance security at the installation entrances and expedite access for personnel and vehicles. The purpose of this system is to validate credentials against authoritative databases in near real time; personnel will require DoD ID cards to register

with AIE to gain access. The AIE system leverages technology to increase security for the soldiers, family members, DoD civilians, retirees, contract employees, and guests of the installation. One of the primary purposes of establishing the AIE system is to reduce potential human errors that can occur at access points, such as missing expired identification or knowing if a driver has restricted access. Card holders will drive up to an AIE pedestal and swipe the ID card at a scanner. Once the card is read, the individual's credentials will be validated against federal and state installation records. Installation security personnel will be monitoring the information retrieved from the ID cards and once it is verified, access to the installation or facility will be granted or denied.

7.5 GII OneView – (Endpoint Data Sharing System)

GII OneView is a secure, web-based, geospatial visualization application that allows individual users to view and interact with data and application services within the DHS Geospatial Information Infrastructure (GII). OneView users can add external data sources to their view in common web service formats (KML, KMZ, WMS, and GeoRSS). Other capabilities within OneView include basic attribute query, measurement, location (geocoding, reverse geocoding, and gazetteer), and routing tools. Geospatial information provides a key connection across homeland security-specific missions. OneView delivers the visualization and analytic tools to support the mission stakeholders in their efforts. With OneView, homeland security partners can establish a comprehensive situational and strategic awareness across the nation to better prepare, prevent, respond, and recover from crisis-related events. Access to OneView is granted to authorized federal, state, and local emergency responders, emergency managers, homeland security officials and other personnel with official infrastructure protection responsibilities, through HSIN. OneView can be accessed from most web-browser systems, enabling its use from both fixed and mobile environments.

7.6 Joint Information Exchange Environment (JIEE) – (Endpoint Data Sharing System)

The JIEE is the National Guard Bureau's system of record for facilitating information sharing and collaboration among the National Guard and its federal and state mission partners during emergency response situations such as natural disasters and special security events. With more than 14,000 users across all 50 U.S. states and four territories, JIEE supports Event & Mission management, Requests for Information (RFIs), Requests for Assistance (RFAs), and geospatial mapping capabilities and data feeds that contribute to the Common Operational Picture (COP) for enhanced situational awareness. JIEE allows the National Guard to act with one voice in support of state and national civilian leadership in times of need. The system has helped coordinate National Guard response efforts for natural disasters such as hurricanes, floods, wildfires, as well as special security events such as the Presidential Inauguration, sporting events, and major exercises.

7.7 Coastal Surveillance System (CSS) – (Endpoint Data Sharing System)

The Department of Homeland Security (DHS) Science and Technology Directorate is improving the ability of the U.S. Coast Guard (USCG), U.S. Customs and Border Protection (CBP), and other DHS operational components to interdict small vessels by developing a

Coastal Surveillance System (CSS). CSS is an open, web-based architecture for rapid technology insertion and agile information sharing. The CSS integrates data feeds from existing local and regional sensors. An unclassified data fusion engine then analyzes the data and provides law enforcement agencies with real-time actionable information, including vessel tracking information. The CSS also provides a secure, service-based framework that can integrate into existing user networks without requiring a redesign of the hardware infrastructure.

7.8 Keystone (DSEA Service available for transition)

In response to the requirement to more efficiently share information without negatively impacting current system investments and emergency management (EM)/force protection (FP) operations, the PSEAG-sponsored Mission Assurance, Threat Alert, Disaster Resiliency and Response (MATADRR) initiative developed a middleware software capability called Keystone. Keystone is based on the Unified Incident Command and Decision Support (UICDS) software. Keystone is a standards-based middleware that receives, translates, and transmits incident related data between linked disparate systems to allow a common view between them. As middleware, Keystone does not interface directly with end users. Keystone is the transporter of uniform data in common formats. Emergency applications (sensors, incident logs, personnel management, dispatch systems, video surveillance and intelligence tools – anything related to homeland security) can provide a portion of their data to Keystone, which then publishes it to subscribers' applications. The applications then see the consumed data inside their own user interface. Thus, to the user, there is no new application, no new learning, and no conscious sending of information. Further, Keystone is not intended to replace current standard operating procedures, messages and/or reports for communicating emergency management and force protection data. It is intended to enhance, enable, and more quickly disseminate EM and FP data to a broader community of recipients. Paramount to Keystone's success is the concept of improved local and regional awareness, with simultaneous national awareness, available to decision makers at all levels in between.

7.9 Physical Security Integration Framework (PSIF) – (End Point Data Sharing System)

The PSIF was developed via the Joint Program Manager–Guardian effort. The framework is a government off-the-shelf (GOTS) tool utilizing disparate technologies to provide an integrated set of capabilities that improve installation-wide situational awareness. The framework allows for both Emergency Operations Center and Incident Command Post operations to synchronize with installation assets and functions, including physical security, emergency management, and force protection. The PSIF is permissions-based, National Incident Management System (NIMS)-compatible, Information Assurance certified, and Common Access Card-enabled. PSIF is an ongoing effort that has a prototype currently deployed at two locations.

8 Stakeholders

8.1 Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs – Nuclear Matters – Physical Security Enterprise and Analysis Group (OASD (NCB/NM) – PSEAG)

The Physical Security Enterprise and Analysis Group mission is led by the Office of the Assistant Secretary of Defense for Nuclear, Chemical and Biological Defense Programs/Nuclear Matters. The mission of PSEAG is to synchronize physical security material requirements to develop, demonstrate and evaluate emerging interoperable Research, Development, Testing and Evaluation (RDT&E) solutions. It focuses on closing DoD-wide capability gaps through investments resulting in programs of record, technology insertions, or commercial off-the-shelf solutions. The PSEAG leverages solutions across nuclear and conventional physical security environments as well as counter nuclear threats.

8.2 Office of the Under Secretary of Defense (Intelligence) – Defense Security Enterprise Advisory Group (OUSD(I) – DSEAG)

The Defense Security Enterprise Advisory Group was created to plan, coordinate, and prioritize decisions for the Defense Security Enterprise Executive Committee (ExCom) as well as establish, oversee, and disband subordinate integrated product teams. The ExCom is the senior-level governance body for the strategic administration and policy coordination of the Defense Security Enterprise (DSE); the DSEAG, in turn, acts to task project teams to research an issue and recommend a plan of action to improve the execution of security functions, as defined by DoD Directive (DoDD) 5200.43.

8.3 Headquarters, U.S. Marine Corps (HQMC)

Headquarters, U.S. Marine Corps, the Service lead for the DSEA, consists of the Commandant of the Marine Corps and those staff agencies that advise and assist him in discharging his responsibilities prescribed by law and higher authority. The United States Marine Corps (USMC) is a branch of the U.S. military responsible for providing power projection from the sea, utilizing the mobility of the U.S. Navy to rapidly deliver combined-arms task forces to global crises.

8.4 U.S. Northern Command (USNORTHCOM) - OM (Operational Manager)

The U.S. Northern Command associates to conduct homeland defense, civil support, and security cooperation to defend and secure the United States and its interests. USNORTHCOM's civil support mission includes domestic disaster relief operations that occur during fires, hurricanes, floods and earthquakes. Additionally, USNORTHCOM support includes counter-drug operations and managing the consequences of a terrorist event employing a weapon of mass destruction.

8.5 Global Combat Support System – Air Force Project Management Office (GCSS-AF PMO) – TM (Technical Manager)

The GCSS-AF program modernizes, consolidates, develops, and integrates Air Force and Department of Defense combat support information systems and provides the warfighter and supporting elements with timely, accurate, and trusted Agile Combat Support (ACS) information.

8.6 Space and Naval Warfare Systems Center Pacific (SSC Pacific) – XM (Transition Manager)

Space and Naval Warfare Systems Center Pacific (SSC Pacific) is the Navy's premier research, development, test, and evaluation (RDT&E) laboratory for command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). Its mission is to enable dominance in information warfare for naval, joint, national, and coalition warfighters through research, development, delivery and support of integrated capabilities. SSC Pacific delivers integrated C4ISR solutions to the nation's warfighters, integrating forces, platforms, and functions into coordinated operational capabilities.

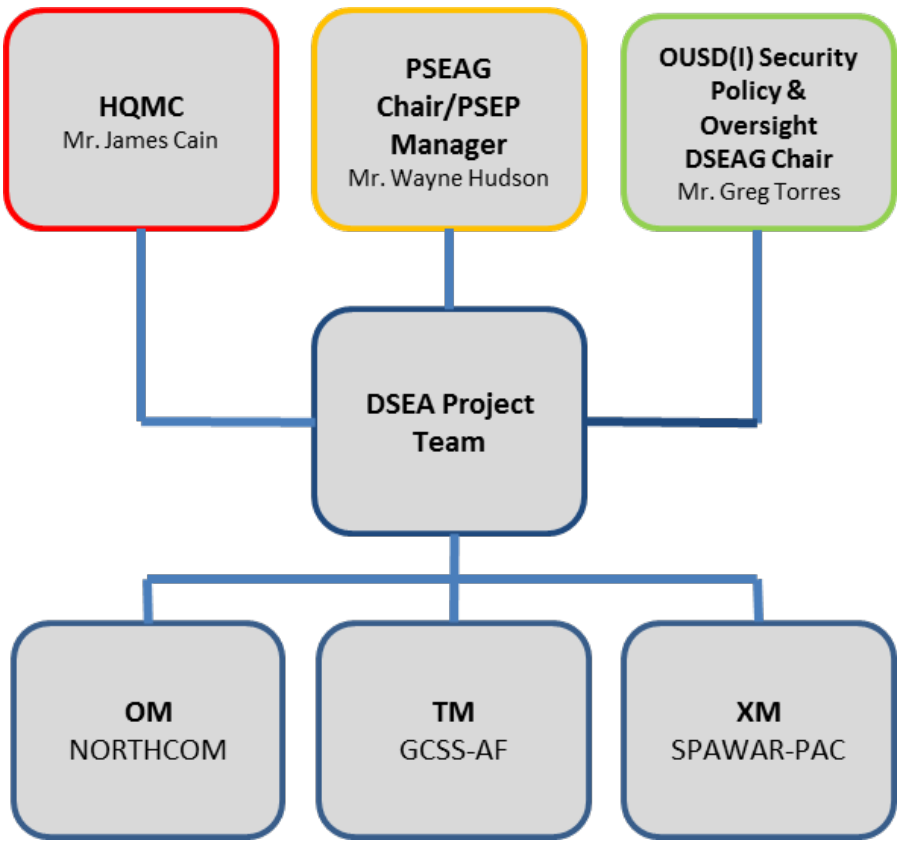


FIGURE 12. DSEA MANAGEMENT STRUCTURE.

9 Transition and Technical Integration Partners

The following are current and proposed technical and transition partners. [At the time of this report, some of the transition efforts are planned or in-progress, and are preceded with a "(Proposed)" in front of the transition description.]

9.1 DTRA Integrated Early Warning (IEW)

- Transition DSEA Product Package via Transition Transmittal Letter
- Technical Integration effort involving WebEOC and C4IS endpoint systems in the DSEA FXD
- IEW is S&T, and as a biological component of the Countering Weapons of Mass Destruction (CWMD) System Constellation, provides the opportunity for the transition of software services to be used in a DTRA program of record (POR) (Constellation), the JPEO-CBD's Biosurveillance Portal, and DTRA's Biosurveillance EcoSystem
- TM is interested in DSEA filling military-civilian gap, e.g., WebEOC, C4IS information sharing
- TM is interested in DSEA components, e.g., EaaS

9.2 JPMIS JWARN, Biosurveillance Portal (BSP)

- Transition DSEA Product Package via Transition Transmittal Letter
- JPMIS has multiple PORs that all or parts of DSEA software services could support
- JPMIS has components on the DISA MilCloud, DSEA ESB services could be migrated to a new hosting environment

9.3 National Guard Bureau (NGB) Joint Information Exchange Environment (JIEE), Mission Partner Environment (MPE)

- Transition DSEA Product Package via Transition Transmittal Letter
- Technical integration effort with JIEE is an endpoint system in the DSEA FXD and is connected to the DSEA ESB for information sharing

9.4 Defense Manpower Data Center (DMDC)

- (Proposed) Transition DSEA Product Package via Transition Transmittal Letter
- Most logical, several common goals with the Origin Network for Identity Exchange (ONIX), services could be provided post-FXD

9.5 Mission Assurance Risk Management System (MARMS)

- (Proposed) Transition DSEA Product Package via Transition Transmittal Letter
- Currently too early, pre-Initial Capabilities Document (ICD), unable to leverage DSEA ESB software services yet

9.6 Defense Information Systems Agency (DISA)

- (Proposed) Transition DSEA Product Package via Transition Transmittal Letter
- Probably makes the most sense as a new Enterprise Information Sharing POR within DISA

9.7 TACOM

- Transition DSEA Product Package via Transition Transmittal Letter
- Technical integration effort demonstrating info sharing between multiple mass notification systems

9.8 PSEAG Defense Security & CBRN Information Sharing Analysis

- PSEAG technical integration effort with monitoring from USNORTHCOM and active participation from DSEA on use case development
- Examining the benefits of information sharing between the defense security and CBRN domains

10 Other Partners

10.1 Department of Homeland Security Chief Information Officer (DHS CIO)

The Department of Homeland Security is strongly committed to ensuring it has the information technology (IT) capabilities it needs to meet the challenges across the homeland security mission space.

10.2 Department of Defense Chief Information Officer (DoD CIO)

DoD CIO is committed to implementing a foundational element of the joint information environment (JIE). It establishes and oversees the DoD enterprise governance processes for the sharing of data, information, and information technology (IT) services. Further, DoD CIO establishes policy, assigns responsibilities, and provides direction for identifying, developing, and prescribing DoD standards for IT systems and issues a security classification guide regarding information-sharing capabilities.

10.3 National Guard Bureau Chief Information Officer (NGB CIO)

NGB CIO is within the National Guard Bureau's Joint Staff Command, Control, Communications, Computers and Chief Information Officer (J6/CIO) Directorate. The J6 establishes policies/procedures, provides advice, and makes recommendations on J6 matters (including CIO and C4) to the Chief, National Guard Bureau for supporting joint military, combatant command, interagency, and Joint Force Headquarters (State) information sharing for the Homeland Security mission.

10.4 Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD HD&ASA)

The Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, or ASD (HD&ASA), is responsible for the supervision of DoD homeland defense activities, defense support of civil authorities, and Western Hemisphere security affairs for the Department of Defense. The position was established by the National Defense Authorization Act for Fiscal Year 2003 (P.L. 107-314, passed 2 December 2002). The ASD (HD&ASA) is

responsible for homeland preparedness, oversight of the two combatant commands that cover North America (USNORTHCOM) and South America (USSOUTHCOM), and the transfer of technologies to homeland security use, pursuant to Section 1401 of the 2003 DOD Authorization Act. The ASD (HD&ASA) reports to the Under Secretary of Defense for Policy.

10.5 U.S. European Command (EUCOM)

The US European Command (EUCOM) is one of nine unified combatant commands of the United States military, headquartered in Stuttgart, Germany. Its area of focus covers multiple countries and territories, including Europe, Russia, Greenland, and Israel. The commander of the United States military in EUCOM simultaneously serves as the Supreme Allied Commander, Europe (SACEUR) within the North Atlantic Treaty Organization (NATO). This allows for a closer relationship between EUCOM and partner nations.

10.6 U.S. Special Operations Command (SOCOM)

The U.S. Special Operations Command synchronizes the planning of special operations and provides Special Operations Forces (SOF) to support persistent, networked and distributed Geographic Combatant Commander (GCC) operations to protect and advance U.S. interests. SOF provides strategic options for U.S. leadership and the GCCs they support through a global network that fully integrates the U.S. military, interagency and international partners.

10.7 U.S. Army North (ARNORTH)

U.S. Army North (ARNORTH) is the Army component of USNORTHCOM which maintains responsibility for operational control of Joint Task Force - Civil Support and Joint Task Force – North. ARNORTH's mission is to conduct homeland defense, civil support operations, and theater security cooperation activities. On order, U.S. Army North commands and controls deployed forces as a joint task force or joint force land component command. ARNORTH is responsible for developing and unifying the military response capability for chemical, biological, radiological, nuclear and high-yield explosives (CBRNE) incidents. Further, the Civil Support Readiness Directorate trains National Guard Weapons of Mass Destruction Civil Support Teams, which are state first responders for chemical, biological, radiological, nuclear or high-yield explosive incidents.

11 Acronyms

TABLE 1. ACRONYMS.

Acronym	Definition
ABIS	Automated Biometric ID System
ACS	Agile Combat Support
ADR	Authoritative Data Repositories
ADS	Authoritative Data Sources
AFB	Air Force Base
AIE	Automated Installation Entry
ARNORTH	US Army North
ASD HD & ASA	Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs
AWOL	Absent Without Official Leave
BOLO	Be On the Look Out
BSP	Biosurveillance Portal
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAC	Common Access Card
CAP	Common Alerting Protocol
CBRNE	Chemical, Biological, Radiological, Nuclear, and High-yield Explosives
CIO	Chief Information Officer
CONOPS	Concept of Operations
CONUS	Continental United States
COP	Common Operational Picture
CRP/CA/L	Contract Role Players, Cultural Advisors, and Linguists
CSS	Coastal Surveillance System
DHS	Department of Homeland Security
DECC	Defense Enterprise Computing Center
DISA	Defense Information Systems Agency
DMDC	Defense Manpower Data Center
DMZ	Demilitarized Zone (related to network security)
DoD	Department of Defense
DoDD	DoD Directive
DoDI	DoD Instructions
DSE	Defense Security Enterprise
DSEA	Defense Security Enterprise Architecture
DSEE	Defense Security Enterprise Environment
DSEAG	Defense Security Enterprise Advisory Group
DTRA	Defense Threat Reduction Agency

TABLE 1. ACRONYMS. (CONTINUED)

Acronym	Definition
EaaS	Entitlements as a Service
EM	Emergency Management
ESB	Enterprise Service Bus
EUCOM	US European Command
ExCom	Executive Committee
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standard
FP	Force Protection
FVR	Facility Verification Request
GCC	Geographic Combatant Commander
GCSS-AF PMO	Global Combat Support System - Air Force Project Management Office
GII	Geospatial Information Infrastructure
GOTS	Government Off-the-Shelf
HAZMAT	Hazardous Material
HQ	Headquarters
HQMC	Headquarters, US Marine Corps
HTTP	Hypertext Transfer Protocol
ID	Identification Data
IEW	Integrated Early Warning
IMESA	Identity Matching Engine for Security Analysis
ISFD	Industrial Security Facilities Database
IT	Information Technology
IUA	Initial Utility Assessment
JCTD	Joint Concept Technology Demonstration
JIATF-S	Joint Interagency Task Force - South
JIE	Joint Information Environment
JIEE	Joint Information Exchange Environment
JPAS	Joint Personnel Adjudicative System
JPMIS	Joint Project Manager Information Systems
JWARN	Joint Warning and Reporting Network
LA/LB	Los Angeles/Long Beach
MARMS	Mission Assurance Risk Management System
MATADRR	Mission Assurance, Threat Alert, Disaster Resiliency and Response
MUA	Military Utility Assessment
NAVAIR	Naval Air Systems Command
NGB	National Guard Bureau
NIEM	National Information Exchange Model

TABLE 1. ACRONYMS. (CONTINUED)

Acronym	Definition
NIMS	National Incident Management System
OASD (NCB/NM)	Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs - Nuclear Matters
OCONUS	Outside the Continental United States
OD	Operational Demonstration
OGA	Other Government Agencies
OM	Operational Manager
OSD	Office of the Secretary of Defense
OSD RDT&E	Office of the Secretary of Defense Research Development Test and Evaluation
OUA	Operational Utility Assessment
OUSD (I)	Office of the Under Secretary of Defense (Intelligence)
PACS	Physical Access Control System
PKI	Public Key Information
PSEAG	Physical Security Enterprise and Analysis Group
PSIF	Physical Security Integration Framework
RDT&E	Research Development Test and Evaluation
REST	Representational State Transfer
SAR	Suspicious Activity Report
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOCOM	US Special Operations Command
SOF	Special Operations Forces
SPAWARSYSCEN-PAC	Space and Naval Warfare Systems Center - Pacific
TA	Transition Agreement
TD	Technical Demonstration
TM	Technical Manager
TRL	Technology Readiness Level
UICDS	Unified Incident Command and Decision Support
US	United States
USG	United States Government
USMC	United States Marine Corps
USNORTHCOM	US Northern Command
USSOUTHCOM	US Southern Command
VPN	Virtual Private Network
WMD	Weapons of Mass Destruction
WSDL	Web Service Definition Language

TABLE 1. ACRONYMS. (CONTINUED)

Acronym	Definition
XM	Transition Manager
XML	Extensible Markup Language
XSL	eXtensible Stylesheet Language

12 Stakeholder and Partner Point of Contact Information

TABLE 2. STAKEHOLDER AND PARTNER POC INFORMATION.

Title	Name	Org	Phone	Email
Program Manager (Sponsor)	Wayne Hudson	OSD/AT&L/NCB/NM	(703) 697-2953	wayne.p.hudson.civ@mail.mil
Operational Manager	Jay Huston	USNORTHCOM S&T	(719) 554-7842	jay.c.huston.civ@mail.mil
Technical Manager	Eric Mertz	USAF AFMC AFLCMC/HNII	(781) 225-6861	eric.mertz.1@us.af.mil
Transition Manager	Doug Hardy	SPAWAR SYSTEMS CENTER – PACIFIC	(619) 553-5410	hardydr@spawar.navy.mil
Service Lead	Tony Pierce	US Marine Corps	(703) 695-7202	charles.a.pierce1@usmc.mil
Policy Sponsor	Carrie Wibben	Office of the Director for Defense Intelligence & Security - OUSD(I)	(703) 692-3758	carrie.l.wibben.civ@mail.mil
For Further Information Contact…	Peggy West	SPAWAR SYSTEMS CENTER – PACIFIC	(619) 553-6899	margaret.f.west.civ@mail.mil

SPAWAR®

Systems Center
PACIFIC

SD 1509
June 2016 • JN 16199
Approved for public release.